AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Devices 1 through 26, described in Attachment A, that are stored at premises controlled by the FBI

Case No. 3:19mj517

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Southern District of Ohio and elsewhere, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

P. Andrew Gragan, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 08/23/2019

Judge's signature

City and state: Dayton, Ohio

Hon. Michael J. Newman, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF DEVICES 1 THROUGH 26, DESCRIBED IN ATTACHMENT A, THAT ARE STORED AT PREMISES CONTROLLED BY THE FBI	Case No. 3:19mj517

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, P. Andrew Gragan, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), Cincinnati Division. I have been employed as a Special Agent with the FBI since May 2016. I have received training in national-security investigations and criminal investigations, and I have conducted investigations related to international terrorism, domestic terrorism, white-collar crimes, drug trafficking, public corruption, firearms and violent crimes. As part of these investigations, I have participated in physical surveillance and records analysis, worked with informants, conducted interviews, served court orders and subpoenas, and executed search warrants.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, officers, and witnesses. This affidavit is

intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched, as described in Attachment A, is:

a. Asus laptop, model: R500A, S/N: D4N0ASIRR0AV168, containing Samsung 500GB 2.5" SSD, S/N: S3PTNB0J920154W, hereinafter Device 1;

b. Dell Inspiron laptop, S/T: 7K6QSJ2, containing Seagate 2TB 2.5" SATA hard drive, S/N: WDZ80S0H, hereinafter Device 2;

c. ZTE N9130 cellular phone, MEID Hex: 99000609364757, S/N: 327B51042630, containing SIM Card # 89011200002017896866, hereinafter Device 3;

d. Samsung Galaxy S7 Edge, model: SM-G935A, no visible identifiers, hereinafter Device 4;

e. Asus laptop, model: UX501J, S/N: G4N0CXIRR05M15A, containing Samsung 512GB NVMe M.2 SSD, model: M2-HPV5120, S/N: S1X1NYAG904184, hereinafter Device 5;

f. Dell Dimension desktop, model: 8300, S/T: 5C46J31, containing Western Digital 250GB IDE hard drive, S/N: WMAL73509048; Seagate 120GB SATA hard drive, S/N: 3JT0YXN9; and Seagate 120GB SATA hard drive, S/N: 3JT0YVK2, hereinafter Device 6;

g. Western Digital 500GB SATA hard drive, S/N: WCASY2780733, hereinafter Device 7;

h. Dell Inspiron 1720 laptop, model: PP22X, S/T: C0JZFG1, containing: Seagate 500GB 2.5" SATA hard drive, S/N: 5VJ36CJB, hereinafter Device 8;

i. Lenovo YOGA laptop, model: 80Y7, S/N: PF17Y69U, containing Samsung 512GB NVMe SSD, S/N: S3RGNE0JB18247, hereinafter Device 9;

j. Seagate 250GB SATA hard drive, S/N: 6RY02B1L, hereinafter Device 10;

k. Seagate 250GB SATA hard drive, S/N: 9VMVXH66, hereinafter Device 11;

l. Seagate 250GB SATA hard drive, S/N: 6RY02FM9, hereinafter Device 12;

m. Seagate 250GB SATA hard drive, S/N: 6RY01WL5, hereinafter Device 13;

n. Western Digital 500GB SATA hard drive, S/N: WCASY2760183, hereinafter Device 14;

o. Western Digital 2TB SATA hard drive, S/N: WMAZA0037184, hereinafter Device 15;

p. Samsung 400GB SATA hard drive, S/N: S0NFJ13P100233, hereinafter Device 16;

q. Seagate 750GB SATA hard drive, S/N: 5QD588WL, hereinafter Device 17;

r. Toshiba 2TB SATA hard drive, S/N: Z2C84H1AS, hereinafter Device 18;

s. Samsung 1000GB 2.5" SATA hard drive, S/N: S314J90F731572, hereinafter Device 19;

t. Fujitsu 160GB 2.5" SATA hard drive, S/N: K611T8A29G5E, hereinafter Device 20;

u. Western Digital 160GB SATA hard drive, S/N: WMAL92523758, hereinafter Device 21;

v. Lian Li desktop computer tower, model: PC-V2000 Plus, containing Toshiba 3TB SATA hard drive, S/N: 85AAVPRGS3VD and Samsung 850 EVO 500GB SSD, S/N: S21HNXAG642319V, hereinafter Device 22;

w. ZT Systems desktop computer, model: 7343Ma, S/N: 203523910005, containing 500GB Western Digital SATA hard drive, S/N: WCASY8096602, hereinafter Device 23;

x. Apple iPhone 7, model: A1778, IMEI:355331088584172, hereinafter Device 24;

y. Apple iPad (4th Gen), model: A1458, Serial: DMQK8NQGF182, hereinafter Device 25;

z. Dell Inspiron 9300 laptop, S/N: J7LYF81, containing Seagate 160GB IDE hard drive, S/N: 5MAD4F85, hereinafter Device 26.

5. The aforementioned devices are also referred to collectively herein as the "Devices." The Devices are currently in the custody of the FBI. The Devices are located at FBI - Cincinnati Division Headquarters, located at 2012 Ronald Reagan Drive, Cincinnati, Ohio 45236, with the exceptions of: (a) Device 4 and Device 24, which are currently located at the FBI Electronic Device Analysis Unit (EDAU), located at Building 27958A, Quantico, Virginia 22135; and (b) Device 25, which is currently located at the FBI Tennessee Valley Regional

Computer Forensics Laboratory (TVRCFL), located at 3334G Wells Road, Redstone Arsenal, Alabama 35808.

6. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On or about August 4, 2019, at approximately 1:00 a.m., Dayton Police Officers responded to an active shooter in the 400 block of East Fifth Street in Dayton, Ohio. Officers observed a male, later identified as **Connor BETTS (BETTS)**, actively engaged in shooting into a crowd of individuals located at the 400 block of East Fifth Street in Dayton, Ohio, a city in the Southern District of Ohio.

8. The Officers were able to return fire towards the suspect in order to stop the threat. Multiple shots were fired, and **BETTS** was killed. At this time ten (10) people, including **BETTS**, are deceased resulting from the shooting, along with multiple individuals injured. The injured were transported to multiple local area hospitals. **BETTS** was located on the scene wearing body-armor and headphones. During a search of the suspect, a black Samsung S8 Active cellular telephone was located in his back pocket. A search warrant from the Dayton Municipal Court was obtained to search the content of this cellular telephone. The phone number (937) 956-3637 was found to be the call number assigned to the phone. Officers were able to identify the weapon as an assault rifle style firearm.

9. In the morning hours of August 4, 2019, the FBI was able to identify the shooter at the scene based on finger prints. The shooter was identified as **BETTS.**

10. On or about August 4, 2019 a Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Firearms Trace was conducted on the firearm used by **BETTS**, further

described as an Anderson AM-15 5.56mm with serial number 18309695. The purchaser was **Connor Stephen BETTS**, with an address of 2250 Creekview Place, Bellbrook, Ohio, date of birth (DOB) of October 28, 1994, and a Social Security Number (SSN) with the last four digits of 6211. Ohio Bureau of Motor Vehicle (BMV) records reflect the same address, DOB, and last four digits of the SSN for **BETTS**.

11. Records obtained from a Dayton area Federal Firearm Licensed dealer included an ATF Form 4473, which based on my training and experience I know is required in order to complete the transaction of purchasing a firearm from a licensed dealer, for an Anderson Mfg model AM-15 receiver with serial number 18309695, which, based on information provided by ATF, was manufactured outside the state of Ohio. The transferee/buyer was listed on the ATF Form 4473 as **Connor Stephen BETTS** with the aforementioned address, DOB, and SSN. **BETTS** provided (937) 956-3637 and cnnrbetts477@gmail.com as his contact information. The transfer of the firearm from the dealer to **BETTS** was completed on April 12, 2019. Based on experience and training, I am aware that Google uses email addresses ending in @gmail.com as the means by which to identify user accounts with Google. Based on my training and experience, I know that Google is a company that offers an operating system for mobile devices and numerous online services, including email.

12. Box 11e of ATF Form 4473 states, "Are you an unlawful user of, or addicted to, marijuana or any depressant, stimulant, narcotic drug, or any other controlled substance? Warning: The use or possession of marijuana remains unlawful under Federal law regardless of whether it has been legalized or decriminalized for medicinal or recreational purposes in the state where you reside." The form contained warnings concerning the consequences of answering the

questions on the form falsely. **BETTS**'s Form 4473 was checked "No" in response to the question in box 11e.

13. Records from the same FFL dealer also showed an ATF Form 4473 for a Taurus Pt.111 G2C 9mm pistol with serial number TLR08219 was purchased by **BETTS** on November 23, 2018. The response to box 11e was checked "No."

14. On or about August 4, 2019, Dayton Police Officers executed a search warrant, issued by the Dayton Municipal Court, on a 2007 Toyota Corolla bearing Ohio license plate number GNM1586. The vehicle was parked near the scene of the shooting and is believed to have been used by **BETTS** for transportation to the scene and for storage of the weapon he used in the shooting. Ohio BMV records show **BETTS**'s father as the registered owner. Among other items, officers recovered a H&R 12 gauge Pardner Pump shotgun.

15. On or about August 4, 2019, an ATF Firearms Trace was conducted on the shotgun, further described as a Hawk Industries Inc. H&R Pardner Pump 12 gauge shotgun with serial number NZ897689. The purchaser was **Connor Stephen BETTS**, with an address of 2250 Creekview Place, Bellbrook, Ohio, date of birth (DOB) of October 28, 1994, and last four of Social Security Number (SSN) 6211, identifying information consistent with the aforementioned BMV and other records.

16. Records obtained from a Dayton-area Federal Firearm Licensed (FFL) dealer included an ATF Form 4473 for a H&R Pardner 12 gauge shotgun with serial number NZ897689. The transferee/buyer listed on the ATF Form 4473 was **Connor Stephen BETTS** with the aforementioned address, DOB, and SSN. **BETTS**'s phone number on the form is the same number listed on the form mentioned in paragraph 10 above. The transfer of the firearm

from the dealer to **BETTS** was completed on June 21, 2019. **BETTS**'s Form 4473 was checked "No" in response to the question in box 11e.

17. On or about August 4, 2019, **BETTS**'s corpse was taken to the Montgomery County Coroner for autopsy. During the autopsy, Dayton Police Officers removed property from the pockets of **BETTS,** including an approximate three inch long black straw with a baggie attached to the end of it by a rubber band. Inside the baggie was a white powder, which the seizing officers, based on their training and experience, believe to be cocaine based on its appearance. The suspected cocaine was submitted to the Miami Valley Regional Crime Lab (MVRCL) for testing. MVRCL reported, on or about August 9, 2019, that the substance was cocaine. On or about August 15, 2019, MVRCL reported finding cocaine, Xanax, and alcohol in **BETTS**'s system.

18. On or about August 4, 2019, the FBI interviewed a friend of **BETTS**, who was with **BETTS** at the scene of the shooting and was shot and wounded by **BETTS**, and who for the purpose of this affidavit will be referred to as C.B. C.B. advised that around July 26 to 28, 2019, **BETTS** indicated to C.B. that he had relapsed with cocaine and it was not interacting well. C.B. also stated that **BETTS** had also invited him to go the range and shoot his AR, which C.B. did not do.

19. On or about August 4, 2019, the FBI and ATF interviewed a friend of **BETTS**, who for the purpose of this affidavit will be referred to as E.K. E.K. identified Snapchat accounts used by **BETTS**. Based on my training and experience, I know that Snapchat is an online messaging application provided by Snap, Inc.

20. On or about August 4, 2019, a large national retail store, with a Federal Firearms License to deal in firearms, provided information to the FBI of weapon purchases made by

BETTS. The weapons are further described as an H&R 1228 Pardner 12 gauge shotgun with serial number NZ682493, purchased on May 31, 2013; a DPMS Panther Arms, Inc, M4 Sportical .223-5.56 caliber rifle, with serial number L4017969, purchased on November 26, 2013; and a Mossberg 702 Plinkster 22LR rifle with serial number EML4019811, purchased on May 3, 2015. Records obtained from the retail store included ATF Form 4473s for all three firearms. Box 11e was checked "No" on all three Form 4473s.

21. On or about August 5, 2019, the FBI interviewed a high school girlfriend of **BETTS**, who for the purpose of this affidavit will be referred to as H.S. H.S. dated **BETTS** off and on in high school. She advised the FBI that **BETTS** had abused a number of drugs, including Adderall, Xanax, cocaine, and marijuana. H.S. indicated that **BETTS** purchased pills and cocaine from a manager at the restaurant **BETTS** worked at that time. H.S. advised that **BETTS** had told others he could sell cocaine to them, and that during 2013 to 2014, **BETTS** talked about having hallucinations and feeling like bugs were under his skin.

22. On or about August 5, 2019, the FBI interviewed another former, but more recent girlfriend of **BETTS**, who for the purpose of this affidavit will be referred to as C.J. C.J. knew **BETTS** since at least January 2019, having been classmates at a local college. C.J. dated **BETTS** from at least March 2019, until they severed their relationship in or about May 2019. C.J. indicated that **BETTS** was previously addicted to methamphetamine and was a recovering meth addict. **BETTS** had told her he quit "cold turkey" after going on vacation with his family and he was unable to obtain illegal narcotics.

23. On or about August 6, 2019, a search warrant, issued by the Dayton Municipal Court, was served to Snap, Inc., regarding a Snapchat account that E.K. had identified as being used by **BETTS**. On the same day, the company responded and provided subscriber information

for the account, including cnnrbetts477@gmail.com as the subscriber's email address, and a phone number (937) 956-3637.

24. On or about August 4 to 7, 2019, the FBI interviewed multiple individuals associated with **BETTS**. A co-worker, who for the purpose of this affidavit will be referred to as N.G., advised he was aware **BETTS** used to have a methamphetamine addiction approximately three years ago. A co-worker, who for the purpose of this affidavit will be referred to as K.G., advised that **BETTS** had told K.G. that he used to have a drug abuse problem during high school. When K.G. asked what type of drugs **BETTS** was abusing, **BETTS** mentioned huffing and cocaine. A bandmate of **BETTS**, who for the purpose of this affidavit will be referred to as J.C., advised that **BETTS** had told J.C. he used to use methamphetamine. A co-worker of **BETTS**, who for the purpose of this affidavit will be referred to as C.W., advised that **BETTS** had done methamphetamine in the past. C.W. believed **BETTS** had been clean for approximately four years. A co-worker of **BETTS**, who for the purpose of this affidavit will be referred to as A.G., believed that **BETTS** had a history of drug abuse. A.G. also advised that **BETTS** had a Twitter account. A.G. showed the interviewers the Twitter account on his phone and indicated that the account was **BETTS**'s Twitter account. Based on my training and experience, I know that Twitter is a social networking website.

25. On or about August 7, 2019, Twitter responded to a search warrant issued by the Dayton Municipal Court for the Twitter account provided to law enforcement by A.G. Pursuant to this warrant, Twitter provided account information, direct messages, IP addresses, and other information. The email address cnnrbetts477@gmail.com was provided as the email for the Twitter account.

26. On or about August 7, 2019, the FBI interviewed an acquaintance of **BETTS**, who for the purpose of this affidavit will be referred to as J.E. J.E. indicated that he and **BETTS** hung out at least once a month from 2014 through 2017. J.E. indicated that **BETTS** was hardly ever sober during this time and used heroin, cocaine, methamphetamine, and prescription narcotics. J.E. said that **BETTS** would often show up to his home "messed up."

27. On or about August 7, 2019, the FBI interviewed a former co-worker of **BETTS**, who for the purpose of this affidavit will be referred to as E.S. E.S. advised that on or about August 2, 2019, at approximately 4:45p.m., **BETTS** came into her place of employment and bought a beer. Before he left, **BETTS** made the comment, "I just popped a xanny, we'll see how it goes." Based on my training and experience, I know that the term "xanny" is often used as street terminology for Xanax, a controlled substance.

28. On or about August 7, 2019, the FBI interviewed an acquaintance of **BETTS**, who for the purpose of this affidavit will be referred to as J.E. J.E. advised that during the timeframe he and **BETTS** were acquainted, which was late 2018, J.E. believed **BETTS** was using various drugs, including cocaine, methamphetamine, heroin, and molly.

29. On or about August 8, 2019, the FBI again interviewed E.K. E.K. informed the FBI that he and **BETTS** had done "hard drugs," marijuana, and acid together four to five times a week during 2014 to 2015.

30. On or about August 8, 2019, the FBI again interviewed E.K. E.K. had purchased the AR upper kit for **BETTS** through the manufacturer's online store. E.K. stated he purchased a 100-round .223 drum magazine for **BETTS** from a website of a gun magazine distributer. E.K. believed **BETTS** sent E.K. a link for the drum magazine on a messaging application. **BETTS** sent E.K. the amount for the purchase price through an online funds transfer, then E.K. ordered

the magazine and had it shipped to his home. **BETTS** also sent E.K links to body armor and to the AR upper kit, and they followed the same process of payment.

31. On or about August 8, 2019, pursuant to a search warrant, issued by the Dayton Municipal Court, access was gained into the Samsung S8 Active recovered from **BETTS**'s person on or about August 4, 2019. Among the files on the phone were files that appeared to be residual emails. One email stated, "Hi c0nn0wg0nel4ter, It looks like someone logged into your account from device 'Samsung Galaxy S8 Active' on July 25, 2019 at 13:30:53 EDT. The login took place somewhere near Centerville, Ohio, United States." It was signed, "Team Snapchat." Another email stated, "Hi c0nn0wg0nel4ter, This email is to notify you that the password for the Snapchat account c0nn0wg0nel4ter has been changed. Thanks, Team Snapchat."

32. On or about August 9, 2019, the FBI interviewed a friend of **BETTS**, who for the purpose of this affidavit will be referred to as J.B. J.B. advised that **BETTS** had a very dark mind and often discussed dark sexual fantasies. J.B. said the majority of these conversations with **BETTS** were online utilizing Snapchat and a social media platform. J.B. said **BETTS** confided with him and openly spoke about the "dark" thoughts on Snapchat and the social media platform. J.B. provided **BETTS**'s Snapchat account.

33. On or about August 12, 2019, the FBI observed a screenshot provided to the FBI of a purported 2012 Facebook post by **BETTS**'s father of an article entitled, "Double Barrel Handgun Means You Only Have To Be Half as Accurate," bearing a picture of part of a handgun. The purported post had the text above the article, "Connor Betts, this one's for you."

34. Between on or about August 4, 2019, and August 20, 2019, the FBI reviewed journals seized by the Dayton Police Department from the home of **BETTS**, pursuant to a search warrant issued by the Dayton Municipal Court. The journals were found by officers in a desk

drawer in **BETTS**'s bedroom on August 4, 2019. In one journal entry, **BETTS** wrote, on or about November 23, 2016, "Now to go rip Terrifyer! Didn't rip, Dad put passcode on his computer. Gonna ask him in the morning." In my training and experience the term "rip" refers to the making or burning of compact discs, often of music, by use of a computer. In another entry, on or about December 14, 2016, **BETTS** wrote, "Got on the old kids computer – found a ton of music I had forgotten about."

35. The Devices are currently in the lawful possession of the FBI. They came into the FBI's possession in the following way: On or about August 4, 2019, Dayton Police Department (DPD) executed a search warrant issued by the Dayton Municipal Court for **BETTS**'s residence, located at 2250 Creekview Place in Bellbrook, Ohio. DPD seized the Devices pursuant to that warrant. The Devices were found in the following locations:

a. Device 1 was found at the foot of the bed in the northeast bedroom;

b. Device 2 was found on the desk in the northeast bedroom;

c. Device 3 was found on the floor in the center east bedroom;

d. Device 4 was found on the bed in the northeast bedroom;

e. Device 5 was found on the kitchen table;

f. Device 6 was found along the east wall in the basement/computer room;

g. Device 7 was found in an Isonix HD dock in the basement/computer room;

h. Device 8 was found next to the chair in the south bedroom;

i. Device 9 was found next to the chair in the south bedroom;

j. Device 10 through Device 21 were found on the top shelf of shelving along the west wall in the basement computer/music room;

k. Device 22 was found under the desk along the north wall in the basement computer/music room;

l. Device 23 was found under the desk along the east wall in the basement computer/music room;

m. Device 24 was found on the desk along the north wall in the basement computer/music room;

n. Device 25 was by the chair in the south bedroom;

o. Device 26 was under the desk along the north wall in the basement computer/music room.

36. The FBI took custody of the devices in order to assist DPD in the execution of that warrant. FBI CART (Computer Analysis Response Team), EDAU, and TVRCFL have imaged or are in the process of imaging the Devices pursuant to the locally issued warrant, but no search of the actual substantive contents has been conducted. Therefore, while the FBI might already have all necessary authority to search and examine the Devices, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Devices will comply with the Fourth Amendment and other applicable laws.

37. Based on my training and experience, I know that drug users frequently use wireless/cellular devices to carry out their activities. They use cellular phones to communicate with their suppliers and associates. It is common for those involved in illicit drug use to have

multiple phones because certain phones may be used only for certain purposes. For instance, a drug user may use one phone to just speak to his supplier, while using a different phone to speak to members of his/her family or others. I also know that drug users commonly text messages suppliers to discuss matters such as meeting locations, prices, and other information needed to carry out the sale of drugs. They commonly store phone numbers for their associates and suppliers in the electronic phone book/contacts list, often under alias or code names.

38. Based on training and experience, I also know that individuals who purchase firearms will often use wireless/cellular telephones, including digital cameras located on their wireless/cellular device, to communicate about the purchase of firearms and to take photographs or videos of themselves, their location, and their firearms, which can be electronically stored on the cellular phone. I also know that computers and tablets are often used to communicate about and facilitate the purchase of firearms, ammunition, and firearms accessories, which can be stored electronically on the device or on external drives, such as USB drives or hard drives.

39. Based on my training and experience, I am familiar with the process by which individuals purchase, obtain, possess, and sell firearms and ammunition, and how they obtain, possess, sometimes grow, and use controlled substances. I know that individuals engaged in these activities often utilize email and other online and social media platforms and websites to communicate, including purchasing and planning the purchase of firearms and drugs, arranging the subsequent sale and distribution of firearms and drugs, and discussing the use thereof. I also know that individuals engaged in illegal activity often maintain multiple email and social media accounts. These individuals access email and other online and social media platforms and websites through electronic devices such as wireless telephones and computers.

40. Based on training and experience, I know that electronic devices present within a residence are often shared or used by multiple individuals within that residence. As discussed above in paragraph 34, journal entries by **BETTS** indicate his use of multiple devices in the house, including his father's computer ("Dad put passcode on his computer. Gonna ask him in the morning") and an "old kids computer" ("Got on the old kids computer computer – found a ton of music I had forgotten about."). Additionally, as discussed in paragraph 33, a Facebook post from **BETTS**'s father indicates that the two used Facebook to communicate regarding firearms. **BETTS** also used email and social media platforms—accessible by wireless telephones and computers—including Twitter and Snapchat. Those social media platforms were registered to his email address, cnnrbetts477@gmail.com, which **BETTS** listed on a ATF Form 4473 when purchasing a firearm. Based on the foregoing, there is probable cause to believe that evidence of the offenses described in paragraph 48 below, as described in Attachment B, will be present within the information contained on the Devices, described in Attachment A, seized from **BETTS**'s residence.

TECHNICAL TERMS

41. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and

from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or

miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media

include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

42. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a computer and/or electronic storage media that can access the internet and store internet history, IP Addresses, communications, photos, documents, and other data, In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

43. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

44. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or

years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

45. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how

the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process.

Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

46. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

47. *Manner of execution.* Because this warrant seeks only permission to examine a Device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

48. Based on the foregoing, I believe there is probable cause to believe that crimes have been committed, namely, violations of 18 U.S.C. § 922(g)(3) (Possession of a firearm by an unlawful user of a controlled substance or by a person addicted to a controlled substance), 18

U.S.C. § 922(a)(6) (false statement regarding firearms), 18 U.S.C. § 924(a)(1)(A) (false statement regarding firearms); 18 U.S.C. § 1001 (false statement), and 21 U.S.C. § 844 (unlawful possession of a controlled substance), and that evidence, contraband, fruits of crime, and instrumentalities of crime will be found in the Devices.

49. This Court has jurisdiction to issue the requested warrant under Rule 41 of the Federal Rules of Criminal Procedure. Specifically, Rule 41(b)(3) provides that "[a]t the request of a federal law enforcement officer or an attorney for the government: a magistrate judge—in an investigation of domestic or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district." "Domestic terrorism" carries the same meaning as set forth in 18 U.S.C. § 2331. Fed.R.Crim.P. 41(a)(2)(D). That provision, in turn, namely, 18 U.S.C. § 2331(5), defines "domestic terrorism" as "activities that—(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended—(i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States." The FBI is conducting a domestic terrorism investigation to determine whether **BETTS**'s shootings on August 4, 2019, in Dayton, Ohio, within the territorial jurisdiction of the United States, and which involved acts dangerous to human life that are a violation of the criminal laws of the United States or of the State of Ohio, was intended to intimate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction and assassination. This requested warrant is part of that investigation.

50. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

P. Andrew Gragan
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on August 23, 2019, in Dayton, Ohio.

HON. MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is as follows (collectively, the "Devices"):

a. Asus laptop, model: R500A, S/N: D4N0ASIRR0AV168, containing Samsung 500GB 2.5" SSD, S/N: S3PTNB0J920154W ("Device 1");

b. Dell Inspiron laptop, S/T: 7K6QSJ2, containing Seagate 2TB 2.5" SATA hard drive, S/N: WDZ80S0H ("Device 2");

c. ZTE N9130 cellular phone, MEID Hex: 99000609364757, S/N: 327B51042630, containing SIM Card # 89011200002017896866 ("Device 3");

d. Samsung Galaxy S7 Edge, model: SM-G935A, no visible identifiers ("Device 4");

e. Asus laptop, model: UX501J, S/N: G4N0CXIRR05M15A, containing Samsung 512GB NVMe M.2 SSD, model: M2-HPV5120, S/N: S1X1NYAG904184 ("Device 5");

f. Dell Dimension desktop, model: 8300, S/T: 5C46J31, containing Western Digital 250GB IDE hard drive, S/N: WMAL73509048; Seagate 120GB SATA hard drive, S/N: 3JT0YXN9; and Seagate 120GB SATA hard drive, S/N: 3JT0YVK2 ("Device 6");

g. Western Digital 500GB SATA hard drive, S/N: WCASY2780733 ("Device 7");

h. Dell Inspiron 1720 laptop, model: PP22X, S/T: C0JZFG1, containing: Seagate 500GB 2.5" SATA hard drive, S/N: 5VJ36CJB ("Device 8");

i. Lenovo YOGA laptop, model: 80Y7, S/N: PF17Y69U, containing Samsung 512GB NVMe SSD, S/N: S3RGNE0JB18247 ("Device 9");

j. Seagate 250GB SATA hard drive, S/N: 6RY02B1L ("Device 10");

k. Seagate 250GB SATA hard drive, S/N: 9VMVXH66 ("Device 11");

l. Seagate 250GB SATA hard drive, S/N: 6RY02FM9 ("Device 12");

m. Seagate 250GB SATA hard drive, S/N: 6RY01WL5 ("Device 13");

n. Western Digital 500GB SATA hard drive, S/N: WCASY2760183 ("Device 14");

o. Western Digital 2TB SATA hard drive, S/N: WMAZA0037184 ("Device 15");

p. Samsung 400GB SATA hard drive, S/N: S0NFJ13P100233 ("Device 16");

q. Seagate 750GB SATA hard drive, S/N: 5QD588WL ("Device 17");

r. Toshiba 2TB SATA hard drive, S/N: Z2C84H1AS ("Device 18");

s. Samsung 1000GB 2.5" SATA hard drive, S/N: S314J90F731572 ("Device 19");

t. Fujitsu 160GB 2.5" SATA hard drive, S/N: K611T8A29G5E ("Device 20");

u. Western Digital 160GB SATA hard drive, S/N: WMAL92523758 ("Device 21");

v. Lian Li desktop computer tower, model: PC-V2000 Plus, containing Toshiba 3TB SATA hard drive, S/N: 85AAVPRGS3VD and Samsung 850 EVO 500GB SSD, S/N: S21HNXAG642319V ("Device 22");

w. ZT Systems desktop computer, model: 7343Ma, S/N: 203523910005, containing 500GB Western Digital SATA hard drive, S/N: WCASY8096602 ("Device 23");

x. Apple iPhone 7, model: A1778, IMEI:355331088584172 ("Device 24");

y. Apple iPad (4th Gen), model: A1458, Serial: DMQK8NQGF182 ("Device 25");

z. Dell Inspiron 9300 laptop, S/N: J7LYF81, containing Seagate 160GB IDE hard drive, S/N: 5MAD4F85 ("Device 26").

The Devices are currently in the custody of the FBI and located at FBI - Cincinnati Division Headquarters, located at 2012 Ronald Reagan Drive, Cincinnati, Ohio 45236, with the exceptions of: (a) Device 4 and Device 24, which are currently located at the FBI Electronic Device Analysis Unit (EDAU), located at Building 27958A, Quantico, Virginia 22135; and (b) Device 25, which is currently located at the FBI Tennessee Valley Regional Computer Forensics Laboratory (TVRCFL), located at 3334G Wells Road, Redstone Arsenal, Alabama 35808.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of:

- **18 U.S.C. § 922(g)(3)**
- **18 U.S.C. § 922(a)(6)**
- **18 U.S.C. § 924(a)(1)(A)**
- **18 U.S.C. § 1001**
- **21 U.S.C. § 844**

and involve **Conner Stephen BETTS** (**BETTS**) since **2013**, including:

a. any information related to the purchase, use, or possession of firearms;

b. any information related to the purchase, use, or sale of controlled substances;

c. any information related to the types, amounts, and prices of controlled substances or firearms purchased, used, or trafficked as well as dates, places, and amounts of specific transactions;

d. any information related to sources of controlled substances or firearms (including names, addresses, phone numbers, or any other identifying information);

e. any information recording **BETTS**'s schedule or travel from 2013 to the present;

f. all bank records, checks, credit card bills, account information, and other financial records.

g. records of Internet Protocol addresses used;

h. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.